

Gateway Email Encryption

It may not be surprising for you to learn that email is not a secure medium of communication; however, it may surprise you to learn just how inherently insecure it really is - how messages you thought were secure that you sent to your contacts, may in fact be open to others to read once it leaves the network email servers, compromising private information.

Securing confidential and private electronic information has become a visible and highly regulated activity. Security requirements set forth by the 1996 Health Insurance Portability & Accountability Act (HIPAA) require Government agencies and Health Care institutions to securely send and receive private information without compromising electronic data.

There are three trends driving the implementation of email encryption:

- **Regulatory Requirements** – Provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) require the Department of Health and Human Services to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers.
- **Managing Business Risk** – With more confidential information exposed on employee computers and in transit over the public Internet, enterprises must develop and deploy completely new security models.
- **Trading Partner Requirements** – Even enterprises that do not have short-term regulatory or business risk issues to manage are coming under increasing pressure from their business partners to ensure that partner information in their possession remains secure.

Features

The State of Utah now offers a seamless and secure way to send secure email to health care providers and other entities requiring confidential and private communications.

Once you have ordered secure email service (see order form for ordering service), you will be able to send secure email to your contacts.

Key features include:

- Ability to send secure email.
- Ability to secure laptop/desktop data.
- Support for secure file transfer.
- Ability to secure email at the client and the gateway.

Please note: Not all State employees will require sending email securely. Email users that should sign up for this service are those users that send PHI data (Protected Health Information), social security numbers, credit card, or other data that could lead to identity theft or cause harm to the person if exposed. Other users that require sending secure data

that should use this service include those that send network sensitive material such as network maps, IP addresses, and other data that should be encrypted.

Benefits

The process is easy to use:

- It is an automatic, transparent encryption solution that provides security.
- Encrypts on demand.
- Protects traffic over standard email systems.
- Does not require client software.
- Enables external partners to access email securely without requiring installation of any new software.

Support

ITS Customer Support provides help to address technical problems related to the secure email process. If you have problems, please contact the ITS Helpdesk at 538-3440.

For the internal users of the State of Utah Email system you will need to go through the following steps to send secure email:

1. Fill out the order form for service activation.
2. After activation, you will simply type sm: before you send a secure mail message. Example in the To: section type "sm:test@yahoo.com" (contact your email administrator if you require further help).
3. Your contact will receive an email message stating that they have received a secure email message. They will then need to click on the link and follow the instructions on how to receive your secure email.

If your partners are experiencing problems with your message after receiving an email from a State of Utah employee, click here (see attached doc that will launch) for instructions on how to use the web email browser.



G:\Project
Management\Active F

(Please add this link to the product webpage)

<http://security.utah.gov/awareness/hipaa/hipaa.htm>